APPENDIX K

INFORMATION TECHNOLOGY (IT) POSITIONS

1. PURPOSE

This appendix establishes standard designations for positions that allow individuals to directly or indirectly affect the operation of unclassified information technology (IT) resources and systems processing unclassified, For Official Use Only (FOUO), and other sensitive information. Such positions are referred to as IT and IT-related positions. These designations are required to distinguish and categorize the impact individuals having certain IT privileges could have on DoD functions and operations.

In today's environment, personnel in nearly every work situation use a computer to perform their assigned duties. In most of these situations, IT systems and resources are used as tools that enhance the incumbent's ability to accomplish their assignments. While these positions may require knowledge of various applications and skill in using available IT resources, the incumbents are not involved in developing, delivering, or supporting IT systems and services, or safeguarding sensitive data within such systems. Such IT users do not occupy IT positions and are not subject to the requirements of this Appendix.

The appendix also includes investigative, adjudicative and due process requirements associated with these positions. The requirements of this appendix, with the exception of Section 10, Adjudication, are to be applied to all IT and IT-related positions, whether occupied by DoD civilian employees, military personnel, consultants, contractor personnel or others affiliated with DoD (e.g., volunteers). Section 10 applies only to contractor personnel.

2. DEFINITIONS

For Official Use Only (FOUO)	DoD information that is not classified CONFIDENTIAL or higher IAW DoD 5200.1-R (reference (q) [revised January 1997]) and that may be withheld from public disclosure IAW DoD 5400.7-R, which implements the Freedom of Information Act (FOIA) (reference (ss)). FOUO information, though unclassified, nonetheless is sensitive and warrants protection from disclosure.
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

DRAFT   DoD 5200.2-R

45	**Limited Privileged Access**	Privileged access with limited scope, e.g., an authority to change
46		user access to data or system resources for a single information
47		system (IS) or physically isolated network.
48		
49	**Non-privileged Access**	User level access, i.e., normal access given to a typical user.
50		Generally, all access to system resources is controlled in a way
51		that does not permit those controls/rules to be changed or
52		bypassed.
53		
54	**Sensitive Information**	Any information the loss, misuse, or unauthorized access to or
55		modification of which could adversely affect the national
56		interest or the conduct of Federal programs, or the privacy to
57		which individuals are entitled under Section 552a of Title 5,
58		United States Code (The Privacy Act), but which has not been
59		specifically authorized under criteria established by executive
60		order or an Act of Congress to be kept secret in the interest of
61		national defense or foreign policy. This includes information in
62		routine DoD payroll, finance, logistics, and personnel
63		management systems. Examples of sensitive information
64		include, but are not limited to, the following categories:
65		

66   (1) **FOUO**: IAW DoD 5400.7-R, information that may be
67   withheld from mandatory public disclosure under the
68   Freedom of Information Act (FOIA) (reference (ss)). See
69   definition above.
70   (2) **Unclassified Technical Data**: Data related to military or
71   dual-use technology which is subject to approval, licenses or
72   authorization under the Arms Export Control Act is
73   withheld from public disclosure IAW DoD 5230.25.
74   (3) **Department of State Sensitive But Unclassified (SBU)**:
75   Information which originated from the Department of State
76   (DoS) which has been determined to be SBU under
77   appropriate DoS information security polices
78   (4) **Foreign Government Information:** Information which
79   originated from a foreign government and which is not
80   classified CONFIDENTIAL or higher but must be protected
81   IAW DoD 5200.1-R (reference (q) [revised January 1997]).
82   **(5) Privacy Data:** Personal and private information (e.g.,
83   individual medical information, home address and telephone
84   number, social security number) as defined in the Privacy
85   Act of 1974 (reference (l)).
86

87	**Privileged Access**	Authorized access that provides capability to alter the
88		properties, behavior or control of the information
89		system/network. It includes, but is not limited to, any of the
90		following types of access:

DRAFT   DoD 5200.2-R

91
92   (1) "Super user," "root," or equivalent access, such as access to
93   the control functions of the information system/network,
94   administration of user accounts, etc.
95   (2) Access to change control parameters (e.g., routing tables,
96   path priorities, addresses) of routers, multiplexers, and other
97   key information system/network equipment or software.
98   (3) Ability and authority to control and change program files,
99   and other users' access to data.
100   (4) Direct access to operating system level functions (also called
101   unmediated access) which would permit system controls to
102   be bypassed or changed.
103   (5) Access and authority for installing, configuring, monitoring
104   or troubleshooting the security monitoring functions of
105   information systems/networks (e.g., network/system
106   analyzers; intrusion detection software; firewalls) or in
107   performance of cyber/network defense operations.
108

3. <u>GENERAL GUIDANCE</u>

110
111   3.1 DoDD 5200.28 (reference (zz)) specifies that information systems/networks shall be
112   safeguarded through use of a mixture of administrative, procedural, physical,
113   communications, emanations, computer, and personnel security measures, that
114   together achieve the requisite level of security. As DoD becomes increasingly
115   dependent upon information technology to execute the DoD mission, ensuring the
116   trustworthiness of all personnel, including temporary, seasonal, and intermittent
117   employees, contractors, and volunteers, in IT positions is critical.
118
119   3.2 The requirements of this appendix are intended to enhance the security of DoD IT
120   systems and networks and to safeguard sensitive information. In those cases where
121   sensitive information (e.g., Privacy Act data) is maintained in contractor owned and
122   operated IT systems that have no interconnection (including data feeds) with DoD IT
123   systems or networks, other safeguards (e.g., non-disclosure agreements, training)
124   authorized in accordance with other applicable guidance may be used at the IT-III
125   level in lieu of background investigations to mitigate the risks associated with the
126   loss/misuse or unauthorized access to or modification of sensitive data.
127
128   3.3 Paragraph 5, below, will help to determine IT position categorization. Other scope
129   and impact factors not specifically identified in paragraph 5 may be considered. Such
130   factors may support changing the category of the position based on the agency's
131   judgement as to the unique characteristics of the information system/network or the
132   safeguards protecting the system/network.
133
134   3.4 Paragraph 5 also provides suggested category assignment by IT specialty. Other
135   categorization schemes exist for IT positions (e.g., the Clinger-Cohen core
136   competencies). This regulation uses Office of Personnel Management's (OPM's) GS-

137   2200A, Information Technology Management series IT specialties because the
138   information and descriptions in the OPM IT classification standard can be easily
139   recognized by both IT personnel and non-IT management who may have to make
140   categorization determinations. Furthermore, the OPM standard, position titles, and
141   associated information are descriptive and use language that can be easily related to
142   position descriptions and personnel requirements.
143

144   3.5 Several factors must be considered to determine the category of an IT position. The
145   most significant factors are: 1) the type of access (privileged or non-privileged), that
146   signifies an incumbent's authorization to effect the operation of DoD information
147   systems and networks, and 2) the potential adverse impact the incumbent could have
148   on the Department's overall security posture or ability to execute its mission. Other
149   factors are the IT specialty, the level of IT knowledge required for effective
150   performance, and the opportunity to affect security and the intended operation or
151   contents of the system/network.
152

153   3.6 Many IT positions involve a mixture of responsibilities and may cover multiple
154   specialty titles. After analysis of a position's aggregated privilege, scope and level of
155   independence, the position should be categorized at the highest level required by the
156   specific duties, risks, and safeguards in place.
157

158   3.7 This policy applies to contractors and consultants in IT and IT-related positions and
159   shall be implemented through incorporation in their contracts.
160

161   3.8 For cases in which the investigative requirements for an IT position exceed the
162   investigative requirements for access to classified information/security clearance
163   requirements, the higher requirement must be met. In such instances, an SF86 will be
164   used.
165

166   3.9 Users of this appendix are also cautioned that other policies may levy additional
167   requirements that must be met prior to assignment to a particular IT-related position.
168   For example, each Designated Approving Authority (DAA), Information System
169   Security Managers (ISSM), and Information System Security Officer (ISSO) must be a
170   U.S. citizen; DAAs additionally must be U.S. Government personnel. Similarly,
171   Verifying Officials (VO) and personnel appointed to operate Certificate Management
172   Authority (CMA) equipment in support of DoD Public Key Infrastructure (PKI) must
173   be U.S. citizens. It is the user's responsibility to be aware of additional requirements
174   pertinent to the specific IT environment and to factor those requirements into this
175   process at the appropriate places.
176

DRAFT   DoD 5200.2-R

177   **4. <u>IT POSITION CATEGORIES</u>**

178

179   This paragraph provides broad guidance for categorizing IT and IT-related positions
180   based on the level of information system/network access required to execute responsibilities of
181   the position and on the potential for adverse impact on the DoD mission. DoD agencies that
182   issue contracts requiring access to DoD IT resources/systems/network shall provide specific
183   guidance to their contractors regarding the categorization of contractor IT positions and the
184   investigative requirements of this regulation.

185

186   4.1 **<u>IT-I Position</u>** – Incumbent of this position has privileged access to networks and
187   information systems, system security and network defense systems, or to system
188   resources; duties are broad in scope and authority, and provide access to the U.S.
189   Government, DoD, or Component mission critical systems. The potential exists for
190   exceptionally serious adverse impact on U.S. Government, DoD, Component or
191   private sector information and/or operations, with worldwide or government-wide
192   effects. Incumbent may also be responsible for unsupervised funds disbursements or
193   transfers or financial transactions totaling over $10M per year.

194

195   4.2 **<u>IT-II Position</u>** – Incumbent of this position has limited privileged access, but duties
196   are of considerable importance to the DoD or DoD Component mission, and the
197   incumbent is under the supervision of an individual in a higher trust position (IT-I).
198   For example, individuals in these positions may have ability to impact a limited set of
199   explicitly defined privileged functions, such as privileged access confined to large
200   portions of an IS or to a local network physically isolated from other DoD or publicly
201   accessible networks. The potential exists for moderate to serious adverse impact on
202   DoD or Component information or operations. Incumbent may also be responsible
203   for monitored/audited funds disbursements or transfers or financial transactions
204   totaling less than $10M per year.

205

206   4.3 **<u>IT-III Position</u>** – Incumbent in this position has non-privileged access to one or more
207   DoD information systems/applications. IT-III incumbents can receive, enter and/or
208   modify information in an information system/application or database to which they
209   are authorized access. Users have access only to that data/information and those
210   applications/networks to which the incumbent is explicitly authorized or has need-to-
211   know and cannot alter those or other users' authorizations. Positive security measures
212   and configuration management ensure that the incumbent can assume only explicitly
213   authorized roles and privileges. The potential exists for limited adverse impact on
214   DoD, Component or unit information or operations. Incumbent may also be
215   responsible for financial operations subject to routine supervision or approval, but has
216   no funds disbursement or transfer capabilities.

217

218   **5. <u>TYPICAL CATEGORY ASSIGNMENT BY IT SPECIALTY</u>**

219

220   5.1 DoD components are responsible for categorization of each IT position at the highest
221   level required by the specific duties, risks, and safeguards in place after analysis of the
222   position's aggregated privileges, scope and levels of independence. Positions may be

223 categorized at higher or lower levels as needed to account for ability to impact overall
224 network/system security posture, intended system behavior, or appropriate content.
225 However, when level of privilege and other position characteristics appear to indicate
226 differing levels of categorization, the higher categorization assignment should be
227 used. Positions in all specialty areas that have greater degrees of management,
228 training or administrative responsibility/duties than technical responsibilities for IT
229 are generally less sensitive than IT positions requiring detailed technical insight or
230 hands-on competency, or positions providing supervision/ oversight of technical
231 positions at a lower categorization. DoD Components may take into consideration
232 existing measures and practices for protecting sensitive information in their
233 impact/risk assessment.

235 5.2 The following are typical category assignments for each IT specialty title defined in
236   the OPM Position Classification Standard "Administrative Work in the Information
237   Technology Group, GS-2200" (http://www.opm.gov/FEDCLASS/gs2200a.pdf).
238   Other IT-related positions should be categorized based on the particular set of duties
239   and responsibilities of the position and the scope, and level of privileges authorized.
240   See also "IT Position Category Assignment Table" below.

242   a. Policy and Planning (PLCYPLN) – IT-III (IT-II if responsible for information
243   security/ information assurance program or if individual also has privileged
244   access)
245   b. Security (INFOSEC) – IT-I (IT-II if primarily policy, planning or awareness
246   focused)
247   c. Systems Analysis (SYSANALYSIS) – IT-III (IT-II if responsible for information
248   security/information assurance systems)
249   d. Applications Software (APPSW) – IT-I, -II, or –III depending on specifics of
250   application (IT-I if responsible for information security/information assurance
251   applications)
252   e. Operating Systems (OS) – IT-II (IT-I if incumbent acts independently, without
253   oversight/review)
254   f. Network Services (NETWORK) – IT-I or IT-II (depending on the scope of
255   network—as defined by criticality of or impact on Department or Federal
256   government mission, geographic reach, and/or major or significant impact on
257   other government agencies and/or the private sector—and level of privileges)
258   g. Data Management (DATAMGT) – IT-III (IT-II if responsible for safeguarding
259   sensitive data/information)
260   h. Internet (INET) – IT-II (IT-I if privileged access to network functions)
261   i. Systems Administration (SYSADMIN) – IT-I (IT-II if stand-alone system or if
262   ability to compromise limited to system/network operation)
263   j. Customer Support (CUSTSPT) – IT-III (IT-I if privileged access; or IT-II if ability
264   to set/change user access privileges (scope and level sensitive))

266 5.3 Other activities or specialties that may have significant IT duties include the
267   following:

268   a. Computer Clerk and Assistant (GS-335) or Computer Operation (GS-332) –
269   typically IT-III, but may be higher if there is access to system/network control
270   functions.
271   b. Telecommunications (GS-391) (e.g., computer network analysts; data
272   communications) – use appropriate IT specialty in paragraph 5.2 above
273   c. Computer engineer (GS-0854) – generally hardware focused; typically IT-III, but
274   specific categorization depends on function and application of the specific
275   hardware/component (e.g., chip/board design may be IT-I), degree of
276   supervision/review by higher authority, etc.
277   d. Computer Science (GS-1550) – categorization depends on specific duties/
278   responsibilities; use appropriate IT specialty in paragraph 5.2 above where
279   possible.
280   e. Criminal Investigating (GS-1811) – Law enforcement activities associated with
281   computer/network crime (e.g., forensic analysis; criminal investigation) –
282   categorization depends upon required level of access (e.g., privileged/non-
283   privileged).
284   f. Miscellaneous Management and Program Analysis (GS-343) and other scientists,
285   subject matter experts, and professionals — depends upon required level of access
286   (e.g., privileged/nonprivileged).
287   g. Technical editors and other subject matter experts who develop web pages, but
288   whose primary expertise is not technical knowledge of Internet systems, services,
289   and technologies – categorize under "Internet" IT specialty; if non-privileged
290   access, may be assigned IT-III designation
291   h. Miscellaneous IT specialists (As required by specifics of new technology/
292   evolving specialty area) – use appropriate IT specialty in paragraph 5.2 above
293   where possible.
294   i. Threat and vulnerability assessment (e.g., red-teams; penetration testing) –
295   determined by the purpose and scope of the assessment objective and required
296   level of access.
297   j. Certificate Management Authorities (CMA) to include Verifying Officials (VO) -
298   typically IT-II, but may be higher if operating CMA equipment associated with
299   Public Key Infrastructure operating above the DoD Class 4 assurance level.
300

DRAFT   DoD 5200.2-R

301   **IT Position Category Assignment Table**

302   *Categorization is based on assessment of the potential adverse impact (e.g.,*
303   *exceptionally serious, moderate to serious, or limited) a typical incumbent could have, given*
304   *the stated combination of IT position characteristics.*
305
306

IT Position Character-istics / **IT Specialist (ITSPEC) Category***	*Privileged Access* − Super User/Root Access to DoD IS *Independence* − Independent of routine supervision	*Limited Privileged Access* − Privileged access with limited scope − Ability to set/change accesses or system resources on single IS or standalone network *Independence* − Subject to periodic/spot super-vision/monitoring/audits by IT-I	*Nonprivileged Access* − User level access to one or more DoD IS − No ability to set or change accesses or system resources *Independence* − Subject to routine review/supervision
Policy and Planning (PLCYPLN)	IT-II	IT-II	IT-III
Security (INFOSEC)	IT-I	IT-I	IT-II
Systems Analysis (SYSANALYSIS)	IT-II	IT-III	IT-III
Applications Software (APPSW)	IT-I	IT-II	IT-III
Operating Systems (OS)	IT-I	IT-II	IT-II
Network Services (NETWORK)	IT-I	IT-I	IT-II
Data Management (DATAMGT)	IT-II	IT-II	IT-III
Internet (INET)	IT-I	IT-II	IT-II
Systems Administration (SYSADMIN)	IT-I	IT-I	IT-II
Customer Support (CUSTSPT)	IT-I	IT-II	IT-III
Other (Miscellaneous IT specialists, management, subject matter experts, etc.—categorization depends upon required level of access)	IT-I	IT-II	IT-III

307
308   * *(as defined by the OPM Position Classification Standard "Administrative Work in the Information Technology Group, GS-2200"*
309   (http://www.opm.gov/FEDCLASS/gs2200a.pdf)*)*

310   **6. ACCESS BY NON-U.S. CITIZENS**

311

312   6.1 Every effort shall be made to ensure that non-U.S. citizens are not employed in IT
313   positions. However, compelling reasons may exist to grant access to DoD IT
314   resources in those circumstances where a non-U.S. citizen possesses a unique or
315   unusual skill or expertise that is urgently needed for a specific DOD requirement and
316   for which a suitable U.S. citizen is not available.

317

318   6.2 Access to sensitive information by a non-U.S. citizen shall only be permitted IAW
319   applicable disclosure policies (e.g. National Disclosure Policy 1, DoDD 5230.9,
320   DoDD 5230.25) and U.S statutes (e.g., Arms Export Control Act). A non-U.S. citizen
321   shall not be assigned to a DoD IT position requiring access to information which is
322   not authorized to be disclosed.

323

324   6.3 Provided that information to which the incumbent will have access is authorized for
325   foreign disclosure, non-U.S. citizens assigned into DoD IT positions are subject to the
326   investigative requirements outlined in paragraph 7.

327

328   6.3.1 Non-U.S. citizens may hold/be authorized access to IT-II and IT-III positions
329   when the conditions described in paragraphs 6.1 and 6.2 exist if the Designated
330   Approving Authority (DAA) approves the assignment in writing. The written
331   approval must be on file before requesting the required investigation. The
332   required investigation must be completed and favorably adjudicated prior to
333   authorizing IT-II and IT-III access to DoD systems/networks. Interim access is
334   not authorized.

335

336   6.3.2 A non-U.S. citizen may be assigned to an IT-I position when the conditions
337   described in paragraphs 6.1 and 6.2 exist and the Head of the DoD Component or
338   Agency that owns the system/information approves the assignment in writing.
339   The written approval must be on file before requesting the required investigation.
340   The required investigation must be completed and favorably adjudicated prior to
341   authorizing IT-I access to DoD systems/networks. Interim access is not
342   authorized.

343

344   **7. LEVEL OF BACKGROUND INVESTIGATION**

345

346   The required investigations for all IT-I, IT-II and IT-III positions are outlined below.

347

Position Category	Civilian	Military	Contractor	Non-U.S. Citizen
IT-1	SSBI	SSBI	SSBI	SSBI, if approval granted
IT-II	NACIC	NACLC	NACLC	NACLC
IT-III	NACIC	NAC	NAC	NAC

348
349

350   Assignment (including assignments due to accretion of duties) of current DoD employees,
351 military personnel, consultants and contractors to positions with different responsibilities or
352 changed access privileges requires verification of the appropriate investigative basis/authority for
353 holding a position of that level of sensitivity.
354
355 **8. REQUESTS FOR INVESTIGATION**
356
357   8.1 All requests for investigations for IT positions that do not require access to classified
358   information shall be initiated using the Questionnaire for Public Trust Positions, SF 85P
359   with Supplemental Questionnaire and SF87/FD 258, Fingerprint Card. The form shall be
360   completed only after a conditional offer of employment.
361
362   8.2 OPM Procedures
363
364   8.2.1   The SF85P and Supplemental Questionnaire (printed form with signed release(s)),
365   FD258 fingerprint card, and Agency Use Block Information attachment (see page
366   K-14) are to be mailed to: U.S. Office of Personnel Management (OPM), Federal
367   Investigations Processing Center, P.O. Box 700, 1137 Branchton Road, Boyers,
368   PA 16018-0700.
369
370   8.2.2   Each submitting office will need to establish a submitting office number (SON)
371   with OPM. To obtain a SON, complete PIPS Form 12 (see page K-15) and fax it
372   to OPM at (724) 794-2891. Your office must place this SON code on each
373   request submitted to OPM.
374
375   8.2.3   When completing the Agency Use Block information, all requests must indicate
376   one of the following central adjudication numbers, as appropriate, in Item L:
377
378   Army ....A334   DIA..............DD08
379   Navy...............NV00   WHS............DD02
380   Air Force ....AF00   OPM............OM25 (contractors only)
381   NSA................SP00
382
383   8.2.4   When completing Item N, indicate the appropriate billing code.
384
385   8.3 For cases in which the investigative requirements for an IT position exceed the
386   investigative requirements for access to classified information, the higher requirement
387   must be met. In such instances, an SF86 will be used.
388
389 **9. INTERIM ASSIGNMENT**
390
391   9.1 Individuals, except non-U.S. citizens, to include temporary, intermittent and seasonal
392   personnel, may be assigned to IT-I, IT-II, and IT-III positions on an interim basis prior
393   to a favorable adjudication of the required personnel security investigation only after
394   the conditions specified below have been met. Interim access is not authorized for
395   non-U.S. citizens.

396
397   9.1.1 **IT-I**:
398   • Favorable completion of the NAC (current within 180 days)
399   • Initiation of an SSBI/favorable review of SF85P and Supplemental
400   Questionnaire
401
402   9.1.2 **IT-II**:
403   • A favorable review of local personnel, base/military, medical, and other
404   security records as appropriate
405   • Initiation of a NACIC (for civilians) or NACLC (for military and contractors),
406   as appropriate/favorable review of SF85P and Supplemental Questionnaire
407
408   9.1.3 **IT-III**:
409   • A favorable review of local personnel, base/military, medical, and other
410   security records as appropriate
411   • Initiation of a NACIC (for civilians) or NAC (for military and contractors), as
412   appropriate/favorable review of SF85P and Supplemental Questionnaire
413
414   9.2 For DoD civilian and military personnel, the approval for interim assignment shall be
415   made by the security manager at the requesting activity. For DoD contractor
416   personnel, the approval shall be made by the government sponsor's security
417   manager/official.
418

419 **10. ADJUDICATION**

420
421   10.1 The provisions of this section apply only to contractor personnel. Civilian employees,
422   military personnel, consultants, volunteers, and seasonal, part-time and intermittent
423   employees will be adjudicated by the appropriate DoD central adjudication facility.
424
425   10.2 All investigations conducted by OPM in accordance with this appendix will be
426   adjudicated by OPM for a trustworthiness determination using the national
427   adjudicative guidelines for access to classified information. If the adjudication is
428   favorable, OPM will issue a letter of trustworthiness to the requesting activity.
429
430   10.3 If a favorable trustworthiness determination cannot be made, OPM will forward the
431   case to the Defense Office of Hearings and Appeals (DOHA) in Columbus, OH, for
432   further processing under DoDD 5220.6. A final unfavorable decision precludes
433   assignment to an IT-I, II, or III position.
434
435   10.4 All OPM IT trustworthiness determinations of DoD contractor personnel will be
436   entered into the OPM Security and Suitability Investigative Index (SII).
437

438 **11. REINVESTIGATION**

439
440   Individuals occupying an IT position shall be subject to a periodic reinvestigation
441   according to prevailing policy.

442

443 **12. PRIOR BACKGROUND INVESTIGATIONS**

444

445   If an individual previously has been subject to background investigative and adjudicative
446 requirements, depending on the age and scope of the investigation those requirements may not
447 need to be duplicated for assignment to an IT position. Investigative criteria for DoD personnel
448 and contractors/consultants who have had prior background investigations are outlined in the
449 table below.

450

451   IT Position Category/Investigative Equivalency Table
452   DoD Civilian and Military Personnel, Contractors, and Consultants

453

If Position Category is:	*Individual has/had the following investigation:*	*And the age of the investigation is:*	*Then the investigation required is:*
IT-I	SSBI	< 5 yrs	None
	SSBI-PR	> 5 yrs	SSBI-PR
	SBI BI LBI MBI NACLC ANACI NAC NACIC ENTNAC	Regardless of age of the investigation	SSBI
IT-II	SSBI SSBI-PR SBI BI LBI MBI NACLC ANACI NACIC	< 10 yrs	None
		> 10 yrs	NACLC
	ENTNAC NAC	Regardless of age of the investigation	NACLC (contractor, military) NACIC (civilian)
IT-III	SSBI SBI BI SSBI-PR LBI MBI ANACI NACLC NACIC ENTNAC NAC	< 15 yrs	None
		> 15 yrs	NAC (contractor, military) NACIC (civilian)

454

455

456 **13. TRAINING AND AWARENESS REQUIREMENTS**

457

458   DoD Components must ensure that individuals performing IT functions within the
459 designated category receive the requisite information assurance, security awareness, and
460 functional competency training. Understanding the threats, system vulnerabilities, and protective
461 measures required to counter such threats are key features to a core information assurance
462 awareness program at each IT position level.